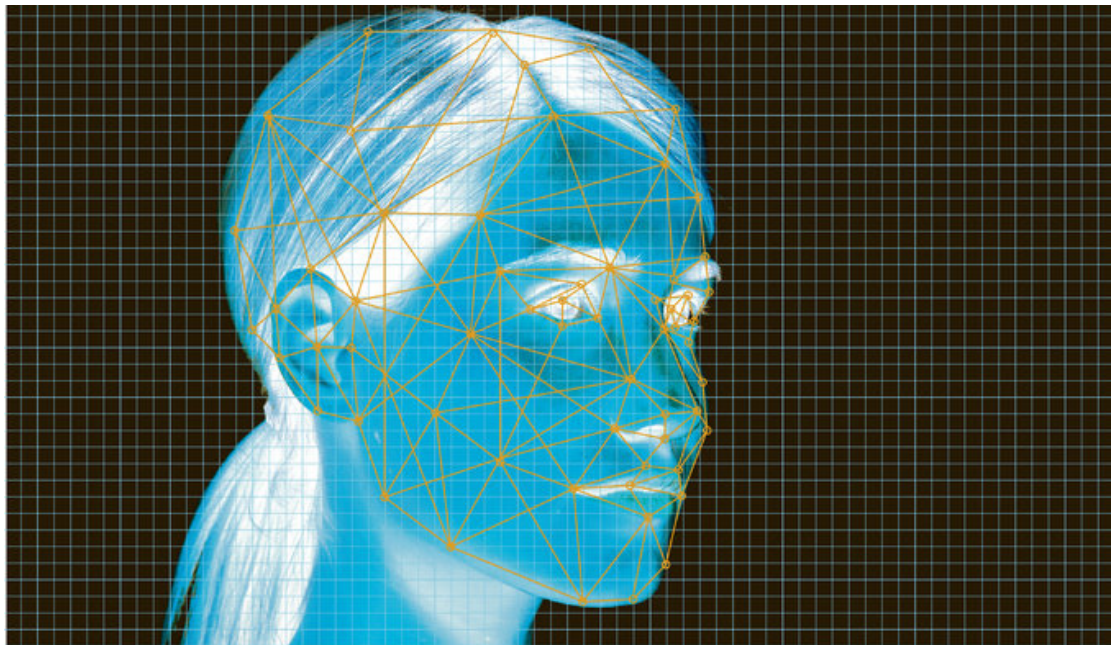
TECHNOLOGY | YOU FOR SALE

Never Forgetting a Face

By NATASHA SINGER MAY 17, 2014

Joseph J. Atick cased the floor of the Ronald Reagan Building and International Trade Center in Washington as if he owned the place. In a way, he did. He was one of the organizers of the event, a conference and trade show for the biometrics security industry. Perhaps more to the point, a number of the wares on display, like an airport face-scanning checkpoint, could trace their lineage to his work.



A physicist, Dr. Atick is one of the

Minh Uong/The New York Times

pioneer entrepreneurs of modern face recognition. Having helped advance the fundamental face-matching technology in the 1990s, he went into business and promoted the systems to government agencies looking to identify criminals or prevent identity fraud. “We saved lives,” he said during the conference in mid-March. “We have solved crimes.”

Thanks in part to his boosterism, the global business of biometrics — using people’s unique physiological characteristics, like their fingerprint ridges and facial features, to learn or confirm their identity — is booming. It generated an estimated $7.2 billion in 2012, according to reports by Frost & Sullivan.

Joseph Atick, a pioneer in the industry, now fears that if face-matching is taken too far, it could allow mass surveillance, “basically robbing everyone of their anonymity.”

Making his rounds at the trade show, Dr. Atick, a short, trim man with an indeterminate Mediterranean accent, warmly greeted industry representatives at their exhibition booths. Once he was safely out of earshot, however, he worried aloud about what he was seeing. What were those companies’ policies for retaining and reusing consumers’ facial data? Could they identify individuals without their explicit consent? Were they running face-matching queries for government agencies on the side?

Now an industry consultant, Dr. Atick finds himself in a delicate position. While promoting and profiting from an

Tony Cenicola/The New York Times

industry that he helped foster, he also feels compelled to caution against its unfettered proliferation. He isn't so much concerned about government agencies that use face recognition openly for specific purposes — for example, the many state motor vehicle departments that scan drivers' faces as a way to prevent license duplications and fraud. Rather, what troubles him is the potential exploitation of face recognition to identify ordinary and unwitting citizens as they go about their lives in public. Online, we are all tracked. But to Dr. Atick, the street remains a haven, and he frets that he may have abetted a technology that could upend the social order.

Face-matching today could enable mass surveillance, "basically robbing everyone of their anonymity," he says, and inhibit people's normal behavior outside their homes. Pointing to the intelligence documents made public by Edward J. Snowden, he adds that once companies amass consumers' facial data, government agencies might obtain access to it, too.

To many in the biometrics industry, Dr. Atick's warning seems Cassandra-like. Face recognition to them is no different from a car, a neutral technology whose advantages far outweigh the risks. The conveniences of biometrics seem self-evident: Your unique code automatically accompanies you everywhere. They envision a world where, instead of having to rely on losable ID cards or on a jumble of easily forgettable — not to mention hackable — passwords, you could unlock your smartphone or gain entry to banks, apartment complexes, parking garages and health clubs just by showing your face.

Dr. Atick sees convenience in these kinds of uses as well. But he provides a cautionary counterexample to make his case. Just a few

months back, he heard about NameTag, an app that, according to its news release, was available in an early form to people trying out Google Glass. Users had only to glance at a stranger and NameTag would instantly return a match complete with that stranger's name, occupation and public Facebook profile information. "We are basically allowing our fellow citizens to surveil us," Dr. Atick told me on the trade-show floor.

(His sentiments were shared by Senator Al Franken, Democrat of Minnesota and chairman of the Senate subcommittee on privacy, technology and the law. Concerned that NameTag might facilitate stalking, Mr. Franken requested that its public introduction be delayed; in late April, the app's developer said he would comply with the request. Google has said that it will not approve facial recognition apps on Google Glass.)

Dr. Atick is just as bothered by what could be brewing quietly in larger companies. Over the past few years, several tech giants have acquired face-recognition start-up businesses. In 2011, Google bought Pittsburgh Pattern Recognition, a computer vision business developed by researchers at Carnegie Mellon University. In 2012, Facebook bought Face.com, an Israeli start-up.

Google and Facebook both declined to comment for this article about their plans for the technology.

Dr. Atick says the technology he helped cultivate requires some special safeguards. Unlike fingerprinting or other biometric techniques, face recognition can be used at a distance, without people's awareness; it could then link their faces and identities to the many pictures they have put online. But in the United States, no specific federal law governs face recognition. A division of the Commerce Department is organizing a meeting of industry representatives and

consumer advocates on Tuesday to start hammering out a voluntary code of conduct for the technology's commercial use.

Dr. Atick has been working behind the scenes to influence the outcome. He is part of a tradition of scientists who have come to feel responsible for what their work has wrought. "I think that the industry has to own up," he asserts. "If we do not step up to the plate and accept responsibility, there could be unexpected apps and consequences."

'Not an Innocent Machine'

A few uses of face recognition are already commonplace. It's what allows Facebook and Google Plus to automatically suggest name tags for members or their friends in photographs.

And more applications could be in the works. Google has applied for a patent on a method to identify faces in videos and on one to allow people to log on to devices by winking or making other facial expressions. Facebook researchers recently reported how the company had developed a powerful pattern-recognition system, called DeepFace, which had achieved near-human accuracy in identifying people's faces.

But real-time, automated face recognition is a relatively recent phenomenon and, at least for now, a niche technology. In the early 1990s, several academic researchers, including Dr. Atick, hit upon the idea of programming computers to identify a face's most distinguishing features; the software then used those local points to recognize that face when it reappeared in other images.

To work, the technology needs a large data set, called an image gallery, containing the photographs or video stills of faces already identified by name. Software automatically converts the topography of

each face in the gallery into a unique mathematical code, called a faceprint. Once people are faceprinted, they may be identified in existing or subsequent photographs or as they walk in front of a video camera.

The technology is already in use in law enforcement and casinos. In New York, Pennsylvania and California, police departments with face-recognition systems can input the image of a robbery suspect taken from a surveillance video in a bank, for instance, and compare the suspect's faceprint against their image gallery of convicted criminals, looking for a match. And some casinos faceprint visitors, seeking to identify repeat big-spending customers for special treatment. In Japan, a few grocery stores use face-matching to classify some shoppers as shoplifters or even "complainers" and blacklist them.

Whether society embraces face recognition on a larger scale will ultimately depend on how legislators, companies and consumers resolve the argument about its singularity. Is faceprinting as innocuous as photography, an activity that people may freely perform? Or is a faceprint a unique indicator, like a fingerprint or a DNA sequence, that should require a person's active consent before it can be collected, matched, shared or sold?

Dr. Atick is firmly in the second camp.

His upbringing influenced both his interest in identity authentication and his awareness of the power conferred on those who control it. He was born in Jerusalem in 1964 to Christian parents of Greek and French descent. Conflict based on ethnic and religious identity was the backdrop of his childhood. He was an outsider, neither Jewish nor Muslim, and remembers often having to show an identity booklet listing his name, address and religion.

“As a 5- or 6-year old boy, seeing identity as a foundation for trust, I think it marked me,” Dr. Atick says. To this day, he doesn’t feel comfortable leaving his New York apartment without his driver’s license or passport.

After a childhood accident damaged his eyesight, he became interested in the mechanics of human vision. Eventually, he dropped out of high school to write a physics textbook. His family moved to Miami, and he decided to skip college. It did not prove a setback; at 17, he was accepted to a doctoral program in physics at Stanford.

Aharon Zeevi Farkash, the founder of FST Biometrics, demonstrates how his company’s technology can identify people from their appearance and movements. By Ozier Muhammad on May 17, 2014.

Still interested in how the brain processes visual information, he started a computational neuroscience lab at Rockefeller University in Manhattan, where he and two colleagues began programming computers to recognize faces. To test the accuracy of their algorithms,

they acquired the most powerful computer they could find, a Silicon Graphics desktop, for their lab and mounted a video camera on it. They added a speech synthesizer so the device could read certain phrases aloud.

As Dr. Atick tells it, he concluded that the system worked after he walked into the lab one day and the computer called out his name, along with those of colleagues in the room. “We were just milling about and you heard this metallic voice saying: ‘I see Joseph. I see Norman. I see Paul,’ ” Dr. Atick recounts. Until then, most face recognition had involved analyzing static images, he says, not identifying a face amid a group of live people. “We had made a breakthrough.”

The researchers left academia to start their own face-recognition company, called Visionics, in 1994. Dr. Atick says he hadn’t initially considered the ramifications of their product, named FaceIt. But when intelligence agencies began making inquiries, he says, it “started dawning on me that this was not an innocent machine.”

He helped start an international biometrics trade group, and it came up with guidelines like requiring notices in places where face recognition was in use. But even in a nascent industry composed of a few companies, he had little control.

In 2001, his worst-case scenario materialized. A competitor supplied the Tampa police with a face-recognition system; officers covertly deployed it on fans attending Super Bowl XXXV. The police scanned tens of thousands of fans without their awareness, identifying a handful of petty criminals, but no one was detained.

Journalists coined it the “Snooper Bowl.” Public outrage and congressional criticism ensued, raising issues about the potential intrusiveness and fallibility of face recognition that have yet to be

resolved.

Dr. Atick says he thought this fiasco had doomed the industry: “I had to explain to the media this was not responsible use.”

Then, a few months later, came the Sept. 11 terrorist attacks. Dr. Atick immediately went to Washington to promote biometrics as a new method of counterterrorism. He testified before congressional committees and made the rounds on nightly news programs where he argued that terrorism might be prevented if airports, motor vehicle departments, law enforcement and immigration agencies used face recognition to authenticate people’s identities.

“Terror is not faceless,” he said in one segment on ABC’s “World News Tonight.” “Terror has measurable identity, has a face that can be detected through technology that’s available today.”

It was an optimistic spin, given that the technology at that early stage did not work well in uncontrolled environments.

Still, Dr. Atick prospered. He merged his original business with other biometrics enterprises, eventually forming a company called L-1 Identity Solutions. In 2011, Safran, a military contractor in France, bought the bulk of that company for about $1.5 billion, including debt.

Dr. Atick had waited 17 years for a cash payout from his endeavors; his take amounted to tens of millions of dollars.

In fact, some experts view his contribution to the advancement of face recognition as not so much in research but in recognizing its business potential and capitalizing on it.

“He actually was one of the early commercializers of face-recognition algorithms,” says P. Jonathon Phillips, an electronics engineer at the

National Institute of Standards and Technology, which evaluates the accuracy of commercial face-recognition engines.

Ovals, Squares and Matches

At Knickerbocker Village, a 1,600-unit red-brick apartment complex in Lower Manhattan where Julius and Ethel Rosenberg once lived, the entryways click open as residents walk toward the doors. It is one of the first properties in New York City to install a biometrics system that uses both face and motion recognition, and it is a showcase for FST Biometrics, the Israeli security firm that designed the program.

“This development will make obsolete keys, cards and codes — because your identity is the key,” says Aharon Zeevi Farkash, the chief executive of FST. “Your face, your behavior, your biometrics are the key.”

On a recent visit to New York, Mr. Farkash offered to demonstrate how it worked. We met at the Knickerbocker security office on the ground floor. There, he posed before a webcam, enabling the system to faceprint and enroll him. To test it, he walked outside into the courtyard and approached one of the apartment complex entrances. He pulled open an outer glass door, heading directly toward a camera embedded in the wall near an inner door.

Back in the security office, a monitor broadcast video of the process.

First, a yellow oval encircled Mr. Farkash’s face in the video, indicating that the system had detected a human head. Then a green square materialized around his head. The system had found a match. A message popped up on the screen: “Recognized, Farkash Aharon. Confidence: 99.7 percent.”

On his third approach, the system pegged him even sooner — while he

was opening the outer door.

Mr. Farkash says he believes that systems like these, which are designed to identify people in motion, will soon make obsolete the cumbersome, time-consuming security process at most airports.

“The market needs convenient security,” he told me; the company’s system is now being tested at one airport.

Mr. Farkash served in the Israeli army for nearly 40 years, eventually as chief of military intelligence. Now a major general in the army reserves, he says he became interested in biometrics because of two global trends: the growth of densely populated megacities and the attraction that dense populations hold for terrorists.

In essence, he started FST Biometrics because he wanted to improve urban security. Although the company has residential, corporate and government clients, Mr. Farkash’s larger motive is to convince average citizens that face identification is in their best interest. He hopes that people will agree to have their faces recognized while banking, attending school, having medical treatments and so on.

YOU FOR SALE

Articles in this series examine the business of consumer data.

If all the “the good guys” were to volunteer to be faceprinted, he theorizes, “the bad guys” would stand out as obvious outliers. Mass public surveillance, Mr. Farkash argues, should make us all safer.

Safer or not, it could have chilling consequences for human behavior.

A private high school in Los Angeles also has an FST system. The school uses the technology to recognize students when they arrive — a security measure intended to keep out unwanted interlopers. But it also serves to keep the students in line.

“If a girl will come to school at 8:05, the door will not open and she will be registered as late,” Mr. Farkash explained. “So you can use the system not only for security but for education, for better discipline.”

Faceprints and Civil Liberties

In February, Dr. Atick was invited to speak at a public meeting on face recognition convened by the National Telecommunications and Information Administration. It was part of an agency effort to corral industry executives and consumer advocates into devising a code for the technology’s commercial use.

But some tech industry representatives in attendance were reluctant to describe their plans or make public commitments to limit face recognition. Dr. Atick, who was serving on a panel, seemed to take their silence as an affront to his sense of industry accountability.

“Where is Google? Where is Facebook?” he loudly asked the audience at one point.

“Here,” one voice in the auditorium volunteered. That was about the only public contribution from the two companies that day.

The agency meetings on face recognition are continuing. In a statement, Matt Kallman, a Google spokesman, said the company was "participating in discussions to advance our view that the industry should make sure technology is in line with people's expectations."

A Facebook spokeswoman, Jodi Seth, said in a statement that the company was participating in the process. "Multi-stakeholder dialogues like this are critical to promoting people's privacy," she said, "but until a code of conduct exists, we can't say whether we will sign it."

The fundamental concern about faceprinting is the possibility that it would be used to covertly identify a live person by name — and then serve as the link that would connect them, without their awareness or permission, to intimate details available online, like their home addresses, dating preferences, employment histories and religious beliefs. It's not a hypothetical risk. In 2011, researchers at Carnegie Mellon reported in a study that they had used a face-recognition app to identify some students on campus by name, linking them to their public Facebook profiles and, in some cases, to their Social Security numbers.

As with many emerging technologies, the arguments tend to coalesce around two predictable poles: those who think the technology needs rules and regulation to prevent violations of civil liberties and those who fear that regulation would stifle innovation. But face recognition stands out among such technologies: While people can disable smartphone geolocation and other tracking techniques, they can't turn off their faces.

"Facial recognition involves the intersection of multiple research disciplines that have serious consequences for privacy, consumer protection and human rights," wrote Jeffrey Chester, executive

director of the nonprofit Center for Digital Democracy, in a recent blog post.

“Guidelines at this stage could stymie progress in a very promising market, and could kill investment,” Paul Schuepp, the chief executive of Animetrics, a company that supplies mobile face-recognition systems to the military, recently wrote on the company’s blog.

Dr. Atick takes a middle view.

To maintain the status quo around public anonymity, he says, companies should take a number of steps: They should post public notices where they use face recognition; seek permission from a consumer before collecting a faceprint with a unique, repeatable identifier like a name or code number; and use faceprints only for the specific purpose for which they have received permission. Those steps, he says, would inhibit sites, stores, apps and appliances from covertly linking a person in the real world with their multiple online personas.

“Some people believe that I am maybe inhibiting the industry from growing. I disagree,” Dr. Atick told me. “ I am helping industry make difficult choices, but the right choices.”

A version of this article appears in print on May 18, 2014, on page BU1 of the New York edition with the headline: Never Forgetting a Face.

SITE INDEX

NEWS

World
U.S.
Politics
New York
Business
Technology
Science
Health
Sports
Education
Obituaries
Today's Paper
Corrections

OPINION

Today's Opinion
Op-Ed Columnists
Editorials
Contributing Writers
Op-Ed Contributors
Opinionator
Letters
Sunday Review
Taking Note
Room for Debate
Public Editor
Video: Opinion

ARTS

Today's Arts
Art & Design
ArtsBeat
Books
Dance
Movies
Music
N.Y.C. Events Guide
Television
Theater
Video Games
Video: Arts

LIVING

Automobiles
Crosswords
Dining & Wine
Education
Fashion & Style
Health
Home & Garden
Jobs
Magazine
N.Y.C. Events Guide
Real Estate
T Magazine
Travel
Weddings & Celebrations

LISTINGS & MORE

Classifieds
Tools & Services
Times Topics
Public Editor
N.Y.C. Events Guide
TV Listings
Blogs
Cartoons
Multimedia
Photography
Video
NYT Store
Times Journeys
Subscribe
Manage My Account

SUBSCRIBE

Times Premier
Home Delivery
Digital Subscriptions
NYT Now
NYT Opinion

Email Newsletters
Alerts
Crosswords
Gift Subscriptions
Corporate Subscriptions
Education Rate

Mobile Applications
Replica Edition
International New York Times